PO Box 5307
Austin, TX 78763-5307
a@aengland.com
512-477-7165
512-322-0211

Anthony England

Fax

To:	USPTO Art Unit 2131	**From:**	Anthony England
Fax:	571-273-3786	**Pages:**	2 (including cover sheet)
Phone:	571-272-3726	**Date:**	May 13, 2008
Attn:	Examiner Kaveh Abrishamkar	**CC:**	

□ **Urgent** □ **For Review** □ **Please Comment** □ **Please Reply** □ **Please Recycle**

Subject: Application Number: 09/940,706
Filing Date: 08-28-2001
Attorney Docket Number: JP920010196US1
Title of Invention: SECURE AUTHENTICATION USING DIGITAL CERTIFICATES

Dear Examiner Abrishamkar,

I received your phone message today. Please find page 3 of the subject patent application attached.

Anthony England

number of services increase, with different versions and types of certificates with the clients and the permutations and combinations of fields the CA would have to take care.

2. Combined Certificates also suffer from the disadvantage of disclosing the entire information of the user to the server, even if it is not required. For example, if a site only implements Secure Email, the user with a combined certificate will still send him all the information including the SET Details (Credit information) which is a security risk.

The object and summary of the invention:

The object of this invention is to obviate the above drawbacks and provide a solution that minimizes security risks.

To achieve the said objective, this invention provides in a method for providing secure authentication using digital certificates, an improvement to enable the selective transfer of authentication data comprising:

- presentation of basic authentication data certified by an accepted certifying authority, at the commencement of a secure transaction,
- transfer of additional individual authentication data units against specific requests, as and when required,

thereby eliminating the risks associated with providing any authentication data that is not required for a particular transaction.

The authenticity of said additional individual authentication data is established by using the public key provided in said basic authentication data.

The authenticity of said additional individual authentication data is established by signature of said accepted certifying authority.

The said additional individual authentication data is provided without the need for establishing a separate session.

The above improved method further comprises the facility to invalidate previously presented